

หลักการและเหตุผล:

สถานการณ์โลกปัจจุบันทำให้ระบบเศรษฐกิจและสังคมเกิดความเปลี่ยนแปลงขึ้นมากมาย พฤติกรรมการใช้ชีวิตประจำวันของผู้คนและการดำเนินธุรกิจต่างเปลี่ยนแปลงไป โลกได้ก้าวเข้าสู่ยุคระบบเศรษฐกิจและสังคมดิจิทัลอย่างเห็นได้ชัด เทคโนโลยีดิจิทัลไม่ได้เป็นเพียงแค่เครื่องมือสนับสนุนการทำงานอีกต่อไป ผู้คนจำนวนมากอาศัยเทคโนโลยีดิจิทัลบนระบบออนไลน์เป็นช่องทางหลักเพื่อใช้ติดต่อสื่อสารแลกเปลี่ยนข้อมูลและประกอบธุรกรรมกันตลอดเวลา เห็นได้จากปริมาณการสั่งซื้อสินค้าและอาหารผ่านช่องทางออนไลน์กันอย่างมากมาย แม้กระทั่งรูปแบบการปฏิบัติงานของบุคลากรขององค์กรก็ปรับเปลี่ยนไปเช่นกัน องค์กรต่างยินยอมให้บุคลากรของตนเองสามารถปฏิบัติงานจากที่บ้านได้ (Work From Home) โดยอาศัยเครือข่ายอินเทอร์เน็ตเป็นช่องทางออนไลน์เชื่อมต่อเข้าสู่ระบบเครือข่ายภายในของแต่ละองค์กรจากที่พำนักของผู้คนเพื่อเข้าถึงระบบงานต่างๆ (Applications) ขององค์กร หรือเพื่อทำการประชุมทางไกลผ่านระบบออนไลน์ (Video Conference) หรือเพื่อประโยชน์อื่นๆอีกมากมาย ผู้ประกอบการทุกภาคธุรกิจและหน่วยงานภาครัฐต่างได้พากันคิดค้นพัฒนาแอปพลิเคชันสำหรับใช้งานบนระบบออนไลน์เพื่ออำนวยความสะดวกและสนองตอบพฤติกรรมของผู้บริโภคที่แปรเปลี่ยนไป จนเป็นที่คาดการณ์เอาไว้ว่าหลังจากนี้ไปการใช้งานแอปพลิเคชันบนระบบออนไลน์จะกลายเป็นส่วนหนึ่งของ New Normal

แต่ด้วยความเจริญก้าวหน้าของเทคโนโลยีดิจิทัลและระบบการสื่อสารออนไลน์ในปัจจุบันที่ได้เปลี่ยนแปลงอย่างรวดเร็วทำให้เทคโนโลยีมีความหลากหลายทวีความซับซ้อนขึ้นกว่าเดิม และหลายองค์กรต่างรีบเร่งพัฒนาแอปพลิเคชันเพื่อตอบสนองต่อความต้องการของผู้ใช้งาน ส่งผลให้ผู้พัฒนาระบบและผู้ใช้งานส่วนใหญ่ขาดทักษะความเข้าใจที่เกี่ยวข้องกับเทคโนโลยีที่นำมาใช้งาน และที่สำคัญคือการขาดความรู้ความเข้าใจ ขาดความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศขององค์กรที่นับได้ว่าเป็นทรัพย์สินที่มีค่ายิ่งต่อองค์กร ทั้งข้อมูลส่วนบุคคลและข้อมูลสำหรับดำเนินกิจการขององค์กร เดิมทีระบบงานส่วนใหญ่ขององค์กรผู้ใช้งานจะสามารถเข้าถึงระบบงานได้จากภายในองค์กรหรือมีการจำกัดสถานที่เพื่อเข้าใช้งานได้เท่านั้น แต่ด้วยสถานการณ์ปัจจุบันองค์กรต่างๆได้ยินยอมให้บุคลากรสามารถปฏิบัติงานจากที่บ้านได้ (Work From Home) จึงทำให้ระบบงานต่างๆ ซึ่งบางระบบงานมีความสำคัญมากต่อองค์กรแต่กลับต้องอนุญาตให้สามารถเข้าใช้ระบบงานเหล่านั้นได้จากสถานที่ไหนก็ได้จากภายนอกองค์กร ทำให้องค์กรต้องเผชิญกับสถานะเสี่ยงต่อการถูกคุกคาม ทั้งปัญหาการถูกคุกคามความปลอดภัยจากภายในองค์กร และการถูกคุกคามทางไซเบอร์ จนก่อให้เกิดความเสียหายจากการละเมิดเพื่อลวงรู้ข้อมูลที่เป็นความลับ ละเมิดเพื่อแก้ไขและทำลายข้อมูล การกระทำทุจริต และภัยคุกคามอื่นๆ ติดตามมาอย่างมากมาย ทำให้องค์กรได้รับความเสียหายทั้งในรูปของเงิน การถูกฟ้องร้อง การเสื่อมเสียชื่อเสียงและความน่าเชื่อถือ โดยผู้คุกคามอาศัยช่องโหว่หรือจุดอ่อนในรูปแบบต่างๆ จากการเข้าใช้งานแอปพลิเคชัน หรือจากการเชื่อมต่อระบบเครือข่ายภายในขององค์กรกับระบบออนไลน์จากภายนอก และโดยการแสวงหาประโยชน์จากช่องโหว่ จุดอ่อนและสถานะเสี่ยงที่มีอยู่ในรูปแบบต่างๆ อีกมากมาย จึงนับเป็นปัญหาสำคัญที่ท้าทายองค์กรว่าจะสามารถรับมือกับเหตุการณ์ที่ไม่พึงประสงค์เพื่อปกป้องรักษาสารสนเทศอันเป็นสินทรัพย์ที่มีมูลค่าและมีความสำคัญต่อการดำเนินภารกิจขององค์กรให้รอดพ้นจากการถูกคุกคามทางไซเบอร์ได้อย่างไร

อย่างไรก็ดี หากองค์กรมีบุคลากรที่มีความรู้ความเข้าใจและมีระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศ มีกระบวนการบริหารจัดการความเสี่ยง มีการควบคุม การติดตาม การตรวจสอบ การวิเคราะห์และการประเมินการจ้างระบบสารสนเทศขององค์กรที่มีประสิทธิภาพ ประสิทธิผลเพียงพอและต่อเนื่องตามมาตรฐาน ISO/IEC 27001 และผู้ปฏิบัติสามารถปฏิบัติตามวัตถุประสงค์ของการควบคุมการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศตามที่องค์กรได้กำหนดไว้ก็จะช่วยให้องค์กรสามารถลดความเสี่ยงของแต่ละโอกาสที่จะถูกคุกคามหรือถูกโจมตีให้เกิดความเสียหาย หรือหากเกิดความเสียหายขึ้นในขนาดขนาดของความเสี่ยงที่จะเกิดขึ้นก็จะอยู่ในระดับที่องค์กรยอมรับได้และไม่ก่อให้เกิดเป็นอุปสรรคต่อการดำเนินภารกิจขององค์กร

ในหลักสูตรนี้ผู้เข้ารับการอบรมจะได้รับความรู้ ความเข้าใจถึงหลักการจัดการการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศในเชิงรุก ด้วยกระบวนการติดตาม การตรวจสอบและการประเมินระบบควบคุมการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศในปัจจุบันขององค์กร เพื่อเปรียบเทียบกับระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศตามมาตรฐาน ISO/IEC 27001 ซึ่งจะช่วยให้องค์กรสามารถทราบได้ว่ามีช่องโหว่ จุดอ่อนอะไรบ้างที่ยังไม่ได้ถูกควบคุม หรือควรทำการปรับปรุงการควบคุมที่มีอยู่เดิมในปัจจุบันอย่างไรบ้าง ทั้งนี้เพื่อให้สามารถควบคุมการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศขององค์กรได้อย่างมีประสิทธิภาพ และเกิดความยั่งยืน จากกรณีศึกษาที่ผ่านการปฏิบัติงานจริงเพื่อให้ผู้เข้ารับการอบรมได้เกิดความรู้ความเข้าใจมากยิ่งขึ้นและสามารถนำไปปฏิบัติได้จริง

วัตถุประสงค์:

- เพื่อให้มีความรู้ ความเข้าใจและตระหนักถึงภัยคุกคามต่อความมั่นคงปลอดภัยทางไซเบอร์
- เพื่อให้มีความรู้ ความเข้าใจเกี่ยวกับระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศ
- เพื่อให้มีความรู้ ความเข้าใจในการควบคุมการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศตามมาตรฐาน ISO/IEC 27001
- เพื่อให้มีความรู้ ความเข้าใจในกระบวนการติดตามและตรวจสอบเพื่อประเมินผลการควบคุมการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศหลังจากนำไปใช้งาน
- เพื่อให้มีความรู้ ความเข้าใจในกระบวนการปรับปรุงการควบคุมการรักษาความมั่นคงปลอดภัยกับระบบสารสนเทศขององค์กรให้เกิดประสิทธิผลมากยิ่งขึ้น

หลักสูตรนี้เหมาะสำหรับ:

- ผู้บริหารหรือผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
- ผู้บริหารหรือผู้จัดการด้านความมั่นคงปลอดภัยสารสนเทศ
- ผู้ที่ทำหน้าที่รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ผู้ที่ทำหน้าที่บริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบภายใน

เนื้อหาหลักสูตร:

- 1. The Overview of Information Security Management Systems (ISMS)**
- 2. Threats of Cyber Security**
- 3. Why is it Necessary to Control and Audit Cyber Security?**
- 4. The Control Sets of ISO 27001**
- 5. How to Controls and Audit Information Security Policies**
 - 6.1.1 Management Direction for Information Security
 - 5.1.1 Policies for information security Controls and Audit
 - 5.1.2 Review of the policies for information security Controls and Audit
- 6. How to Controls and Audit Organization of Information Security**
 - 6.2 Internal Organization
 - 6.2.1 Information Security Roles and Responsibilities Control and Audit
 - 6.2.2 Segregation of Duties Control and Audit
 - 6.2.3 Contact with Authorities Control and Audit
 - 6.2.4 Contact with Special Interest Groups Control and Audit
 - 6.2.5 Information Security in Project Management Control and Audit
 - 6.3 Mobile Devices and Teleworking
 - 6.3.1 Mobile Device Policy Control and Audit
 - 6.3.2 Teleworking Control and Audit
- 7. How to Controls and Audit Human Resources Security**
 - 7.1 Prior to Employment
 - 7.1.1 Screening Control and Audit
 - 7.1.2 Terms and Conditions of Employment Control and Audit
 - 7.2 During Employment
 - 7.2.1 Management Responsibilities Control and Audit
 - 7.2.2 Information Security Awareness, Education and Training Control and Audit
 - 7.2.3 Disciplinary Process Control and Audit
 - 7.3 Termination and Change of Employment
 - 7.3.1 Termination or Change of Employment Responsibilities Control and Audit
- 8. How to Controls and Audit Asset Management**
 - 8.1 Responsibility for Assets
 - 8.1.1 Inventory of Assets Controls and Audit
 - 8.1.2 Ownership of Assets Controls and Audit
 - 8.1.3 Acceptable Use of Assets Controls and Audit
 - 8.1.4 Return of Assets Controls and Audit

- 8.2 Classification of Information
 - 8.2.1 Classification of Information Controls and Audit
 - 8.2.2 Labeling of Information Controls and Audit
 - 8.2.3 Handling of Assets Controls and Audit
- 8.3 Media Handling
 - 8.3.1 Management of Removable Media Controls and Audit
 - 8.3.2 Disposal of Media Controls and Audit
 - 8.3.3 Physical Media Transfer Controls and Audit
- 9. How to Controls and Audit Access Control**
 - 9.1 Business Requirements of Access Control
 - 9.1.1 Access Control Policy Controls and Audit
 - 9.1.2 Access to Networks and Network Services Controls and Audit
 - 9.2 User Access Management
 - 9.2.1 User Registration and de-Registration Controls and Audit
 - 9.2.2 User Access Provisioning Controls and Audit
 - 9.2.3 Management of Privileged Access Right Controls and Audit
 - 9.2.4 Management of Secret Authentication Information of Users
 - 9.2.5 Review of User Access Rights Controls and Audit
 - 9.2.6 Removal or Adjustment of Access Rights Controls and Audit
 - 9.3 User Responsibilities
 - 9.3.1 Use of Secret Authentication Information Controls and Audit
 - 9.4 System and Application Access Control
 - 9.4.1 Information Access Restriction Controls and Audit
 - 9.4.2 Secure Log-on Procedures Controls and Audit
 - 9.4.3 Password Management System Controls and Audit
 - 9.4.4 Use of Privileged Utility Programs Controls and Audit
 - 9.4.5 Access Control to Program Source Code Controls and Audit
- 10. How to Controls and Audit Cryptography**
 - 10.1 Policy on the Use of Cryptographic Controls
 - 10.1.1 Policy on the Use of Cryptographic Controls and Audit
 - 10.1.2 Key Management Controls and Audit
- 11. How to Controls and Audit Physical and Environmental Security**
 - 11.1 Secure Areas
 - 11.1.1 Physical Security Perimeter Controls and Audit
 - 11.1.2 Physical Entry Controls and Audit
 - 11.1.3 Securing Office, Rooms and Facilities Controls and Audit
 - 11.1.4 Protecting Against External and Environment Threats Controls and Audit
 - 11.1.5 Working in Secure Areas Controls and Audit
 - 11.1.6 Delivery and Loading Areas Controls and Audit
 - 11.2 Equipment
 - 11.2.1 Equipment Sitting and Protection Controls and Audit
 - 11.2.2 Supporting Utilities Controls and Audit
 - 11.2.3 Cabling Security Controls and Audit
 - 11.2.4 Equipment Maintenance Controls and Audit
 - 11.2.5 Removal of Assets Controls and Audit
- 12. How to Controls and Audit Operational Security**
 - 12.1 Operational Procedures and Responsibilities
 - 12.1.1 Documented Operating Procedures Controls and Audit
 - 12.1.2 Change Management Controls and Audit
 - 12.1.3 Capacity Management Controls and Audit
 - 12.1.4 Separation of Development, Testing and Operational Environments Controls and Audit

- 12.2 Protection From Malware
 - 12.2.1 Controls Against Malware Controls and Audit
- 12.3 Backup
 - 12.3.1 Information Backup Controls and Audit
- 12.4 Logging and Monitoring
 - 12.4.1 Event Logging Controls and Audit
 - 12.4.2 Protection of Log Information Controls and Audit
 - 12.4.3 Administrator and Operator Logs Controls and Audit
 - 12.4.4 Clock Synchronization Controls and Audit
- 12.5 Control of Operation Software
 - 12.5.1 Installation of Software on Operational Systems Controls and Audit
- 12.6 Technical Vulnerability Management
 - 12.6.1 Management of Technical Vulnerabilities Controls and Audit
 - 12.6.2 Restrictions on Software Installation Controls and Audit
- 12.7 Information System Audit Considerations
 - 12.7.1 Information System Audit Controls
- 13. How to Controls and Audit Communications Security**
 - 13.1 Network Security Management
 - 13.1.1 Network Controls
 - 13.1.2 Security of Network Services Controls and Audit
 - 13.1.3 Segregation in Networks Controls and Audit
 - 13.2 Information Transfer
 - 13.2.1 Information Transfer Policies and Procedures Controls and Audit
 - 13.2.2 Agreements on Information Transfer Controls and Audit
 - 13.2.3 Electronic Messaging Controls and Audit
 - 13.2.4 Confidentiality or Non-Disclosure Agreements Controls and Audit
- 14. How to Controls and Audit System Acquisition, Development and Maintenance**
 - 14.1 Security Requirements of Information Systems
 - 14.1.1 Information Security Requirements Analysis and Specification Controls and Audit
 - 14.1.2 Securing Application Services on Public Networks Controls and Audit
 - 14.1.3 Protecting Application Services Transactions Controls and Audit
 - 14.2 Security in Development and Support Processes
 - 14.2.1 Secure Development Policy Controls and Audit
 - 14.2.2 System Change Control Procedures Controls and Audit
 - 14.2.3 Technical Review of Applications After Operating Platform Changes Controls and Audit
 - 14.2.4 Restrictions on Changes to Software Packages Controls and Audit
 - 14.2.5 Secure System Engineering Principles Controls and Audit
 - 14.2.6 Secure Development Environment Controls and Audit
 - 14.2.7 Outsourced Development Controls and Audit
 - 14.2.8 System Security Testing Controls and Audit
 - 14.2.9 System Acceptance Testing Controls and Audit
 - 14.3 Test data
 - 14.3.1 Protection of Test Data Controls and Audit
- 15. How to Controls and Audit Supplier Relationships**
 - 15.1 Information Security in Supplier Relationship
 - 15.1.1 Information Security Policy for Supplier Relationships Controls and Audit
 - 15.1.2 Addressing Security within Supplier Agreement Controls and Audit
 - 15.1.3 Information and Communication Technology Supply Chain Controls and Audit
 - 15.2 Supplier Service Delivery Management
 - 15.2.1 Monitor and Review of Supplier Services Controls and Audit
 - 15.2.2 Managing Changes to Supplier Services Controls and Audit

16. How to Controls and Audit Information security Incident Management

- 16.1 Management of Information Security Incidents and Improvements
 - 16.1.1 Responsibilities and Procedures Controls and Audit
 - 16.1.2 Reporting Information Security Events Controls and Audit
 - 16.1.3 Reporting Information Security Weakness Controls and Audit
 - 16.1.4 Assessment of and Decision on Information Security Events Controls and Audit
 - 16.1.5 Response to Information Security Incidents Controls and Audit
 - 16.1.6 Learning From Incident Security Incidents Controls and Audit
 - 16.1.7 Collection of Evidence Controls and Audit

17. How to Controls and Audit Information Security Aspects of Business Continuity Management

- 17.1 Information Security Continuity
 - 17.1.1 Planning Information Security Continuity Controls and Audit
 - 17.1.2 Implementing Information Security Continuity Management Process Controls and Audit
 - 17.1.3 Verify, Review and Evaluate Information Security Continuity Controls and Audit
- 17.2 Redundancies
 - 17.2.1 Availability of Information Processes Facilities Controls and Audit

18. How to Controls and Audit Compliance

- 18.1 Compliance with Legal and Contractual Requirements
 - 18.1.1 Identification of Applicable Legislation and Contractual Requirements Controls and Audit
 - 18.1.2 Intellectual Property Rights Controls and Audit
 - 18.1.3 Protection of Records Controls and Audit
 - 18.1.4 Privacy and Protection of Personally Identifiable Information Controls and Audit
 - 18.1.5 Regulation of Cryptographic Controls and Audit
- 18.2 Information Security Reviews
 - 18.2.1 Independent Review of Information Security Controls and Audit
 - 18.2.2 Compliance with Security Policies and Standards Controls and Audit
 - 18.2.3 Technical Compliance Review Controls and Audit

19. PDPA (Personal Data Protection Act)

วิทยากร: อาจารย์กีกันต์ ธีรสัตยาพิทักษ์



- วิทยากรรับเชิญ ประจำสถาบันพัฒนาบุคลากรแห่งชาติ

จำนวนชั่วโมงในการฝึกอบรม: 4 วัน (24 ชั่วโมง)

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

กำหนดการอบรม: ตามตารางปฏิทินอบรมประจำปี <https://www.career4future.com/trainingprogram>

ค่าลงทะเบียนอบรม:

ราคา Onsite	ราคา Online
12,000 บาท	10,800 บาท

<p>STEAM⁺ (เฉพาะหลักสูตรนี้) => ผู้ประกอบการที่ส่งบุคลากรเข้ารับการฝึกอบรมในหลักสูตรที่ผ่านการรับรองตามมาตรการ Thailand Plus Package สามารถ "ลดหย่อนภาษีเงินได้ 250%" ของค่าใช้จ่ายในการฝึกอบรมลูกจ้าง ทุกรายละเอียดเพิ่มเติมได้ที่ www.stemplus.or.th</p>	
<p>หมายเหตุ</p> <ul style="list-style-type: none"> • ราคาค่าลงทะเบียนอบรม ไม่รวมภาษีมูลค่าเพิ่ม • เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไม่ใช่ธุรกิจ และไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม • สถาบันฯ เป็นหน่วยงานราชการ ได้รับการยกเว้นไม่ต้องหักภาษี ณ ที่จ่าย 3% • ค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมทางวิชาชีพของบริษัทหรือห้างหุ้นส่วนนิติบุคคล สามารถนำไปลดหย่อนภาษีได้ 200% • ข้าราชการมีสิทธิ์เบิกค่าลงทะเบียนได้ตามระเบียบกระทรวงการคลังและเข้าร่วมอบรมสัมมนาโดยไม่ถือเป็นวันลา • สถาบันฯ ได้มีการปรับรูปแบบการอบรมทุกหลักสูตรให้พร้อมบริการ ทั้ง แบบ Onsite (Classroom) และ แบบ Online 	<ul style="list-style-type: none"> • สถาบันฯ ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร รูปแบบการอบรม ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม • สถาบันฯ ขอสงวนสิทธิ์ ไม่บันทึกภาพ วิดีโอ หรือบันทึกเสียง ตลอดระยะเวลาการอบรม เนื่องจากเป็นลิขสิทธิ์ร่วมระหว่างวิทยากรกับสถาบันฯ และเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล • ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)
<p>รูปแบบการจัดอบรม Online</p> <ul style="list-style-type: none"> • ถ่ายทอดสดในระบบ Online ผ่านโปรแกรม Zoom เพื่อประสิทธิภาพในการเรียน ควรใช้ Internet ที่มีความเสถียร (ไม่แนะนำให้ใช้ Internet ผ่านมือถือ) • จัดตั้งไลน์กลุ่มเพื่อใช้ในการสื่อสารร่วมกันระหว่างวิทยากร ผู้เข้าอบรม และเจ้าหน้าที่ของสถาบันฯ • ส่งไฟล์เอกสารอบรมให้ Download • จัดส่งวุฒิบัตร e-Certificate ภายหลังจบการอบรม 	<p>รูปแบบการจัดอบรม Onsite</p> <ul style="list-style-type: none"> • สถาบันฯ มีการจัดเตรียม เอกสารการอบรม พร้อมอาหารว่าง และอาหารกลางวันให้กับผู้เข้าอบรม • มอบวุฒิบัตรภายหลังจบการอบรม • สถานที่อบรม ห้องอบรม ณ สถาบันพัฒนาบุคลากรแห่งอนาคต อาคาร สวทช. ชั้น 6 ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

ติดต่อสอบถามรายละเอียด

สถาบันพัฒนาบุคลากรแห่งอนาคต (Career for the Future Academy)
73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ 0 2644 8150 ต่อ 81886-7
โทรสาร 0 2644 8150
E-mail: trianing@nstda.or.th
www.career4future.com